EU General Data Protection Regulation (GDPR)
An Implementation and Compliance Guide
Second Edition
IT Governance Privacy Team
EU General Data Protection Regulation (GDPR)

An Implementation and Compliance Guide

Second edition

IT GOVERNANCE PRIVACY TEAM

IT Governance Publishing

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew’s Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

© IT Governance Privacy Team 2016, 2017

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2016 by IT Governance Publishing:

ISBN 978-1-84928-835-4

Second edition published in the United Kingdom in 2017 by IT Governance Publishing:

ISBN: 978-1-84928-946-7

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
ABOUT THE AUTHOR

IT Governance is a leading global provider of IT governance, risk management and compliance expertise, and we pride ourselves on our ability to deliver a broad range of integrated, high-quality solutions that meet the real-world needs of our international client base.

Our privacy team, led by Alan Calder, has substantial experience in privacy, data protection, compliance and information security. This practical experience, and our understanding of the background and drivers for the GDPR, as well as the input of our fast-growing team of consultants and trainers, are combined in this manual to provide the world’s first guide to implementing the new data protection regulation.
**CONTENTS**

**Introduction** ................................................................................................................. 11  
The purpose of the GDPR .................................................................................. 12  
Structure of the Regulation ............................................................................ 13  
Impact on the EU ............................................................................................. 14  
Implementing the GDPR ................................................................................. 15  
Key definitions ................................................................................................. 18  

**Chapter 1: Privacy Compliance Frameworks** .............................................. 23  
Material scope ........................................................................................................ 27  
Territorial scope .................................................................................................... 28  
Governance ........................................................................................................... 30  
Objectives ............................................................................................................. 32  
Key processes ....................................................................................................... 34  
Personal information management systems ............................................. 39  
ISO/IEC 27001:2013 ............................................................................................. 41  
Selecting and implementing a compliance framework ................... 48  
Implementing the framework ............................................................................ 50  

**Chapter 2: Role of the Data Protection Officer** ................................. 53  
Voluntary designation of a Data Protection Officer ..... 58  
Undertakings that share a DPO ......................................................................... 59  
DPO on a service contract .................................................................................. 61  
Publication of DPO contact details .................................................................... 62  
Position of the DPO ............................................................................................. 63  
Necessary resources ........................................................................................... 64  
Acting in an independent manner ................................................................. 66  
Protected role of the DPO ................................................................................. 67  
Conflicts of interest ............................................................................................. 69  
Specification of the DPO .................................................................................... 71  
Duties of the DPO ................................................................................................. 73  
The DPO and the organisation ........................................................................ 78

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Contents

The DPO and the supervisory authority ......................... 79
Data protection impact assessments and risk management ................................................................. 80
In house or contract ......................................................................................................................... 81

Chapter 3: Common Data Security Failures ......................... 83
Personal data breaches ................................................................. 85
Anatomy of a data breach ........................................................ 86
Sites of attack ............................................................................. 87
Securing your information ...................................................... 88
ISO 27001 ....................................................................................... 89
Ten Steps to Cyber Security .................................................... 90
Cyber Essentials ..................................................................... 91
NIST standards ............................................................................. 92
The information security policy ............................................... 93
Assuring information security.................................................... 94
Governance of information security ....................................... 95
Information security beyond the organisation’s borders 96

Chapter 4: Six Data Protection Principles ......................... 98
Principle 1: Lawfulness, fairness and transparency .......... 100
Principle 2: Purpose limitation .............................................. 108
Principle 3: Data minimisation .............................................. 109
Principle 4: Accuracy ................................................................. 111
Principle 5: Storage limitation .............................................. 113
Principle 6: Integrity and confidentiality ......................... 114
Accountability and compliance ............................................ 116

Chapter 5: Requirements for Data Protection Impact Assessments ................................................ 121
Data protection impact assessments ...................................... 123
When to conduct a DPIA ........................................................ 131
Who needs to be involved ......................................................... 136
Data protection by design and by default ............................. 137

Chapter 6: Risk Management and DPIAs ...............142
DPIAs as part of risk management ........................................ 143

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Contents

Data portability ................................................................. 225
Responsibilities of the data controller.............................. 227
Processes and procedures................................................. 228
Options for confirming the requester’s identity.................... 229
Records to examine ............................................................ 232
Time and money ............................................................... 233
Dealing with bulk subject access requests ......................... 234
Right to refusal ................................................................... 235

Chapter 12: Controllers and Processors ................. 236
Data controllers ............................................................... 236
Joint controllers ............................................................... 238
Data processors ............................................................... 239
Controllers that are processors ......................................... 240
Controllers and processors outside the EU ....................... 241
Records of processing ....................................................... 243
Demonstrating compliance ............................................... 247

Chapter 13: Managing Personal Data Internationally .... 249
Key requirements ............................................................ 250
Adequacy decisions ......................................................... 252
Safeguards ....................................................................... 254
Binding corporate rules .................................................... 256
The EU-US Privacy Shield .............................................. 257
Privacy Shield Principles ............................................... 260
Limited transfers ............................................................ 262
Cloud services ............................................................... 262

Chapter 14: Incident Response Management and Reporting .... 265
Notification .................................................................... 266
Events vs incidents .......................................................... 269
Types of incident .............................................................. 270
Cyber security incident response plans ............................. 271
Key roles in incident management .................................... 273

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Contents

Prepare .................................................................................................................. 274
Respond .................................................................................................................. 275
Follow up ............................................................................................................... 277

Chapter 15: GDPR Enforcement .................................................................. 280
  The hierarchy of authorities ........................................................................... 280
  One-stop-shop mechanism ............................................................................. 282
  Duties of supervisory authorities ................................................................... 283
  Powers of supervisory authorities .................................................................. 284
  Duties and powers of the European Data Protection Board.................. 285
  Data subjects’ rights to redress ....................................................................... 286
  Administrative fines ......................................................................................... 288
  The Regulation’s impact on other laws ......................................................... 291

Chapter 16: Transitioning and Demonstrating Compliance .................. 294
  Transition frameworks ....................................................................................... 294
  Transition – understanding the changes from DPD to GDPR ................. 296
  Using policies to demonstrate compliance ................................................... 299
  Codes of conduct and certification mechanisms ......................................... 304

Appendix 1: Index of the Regulation ......................................................... 306
Appendix 2: EU/EEA National Supervisory Authorities .......................... 313
Appendix 3: Implementation FAQs ............................................................... 317
ITG Resources ...................................................................................................... 377
INTRODUCTION

Due to be enforced from 25 May 2018, the European Union’s General Data Protection Regulation (GDPR) will require all data controllers and processors that handle the personal information of EU residents to “implement appropriate technical and organisational measures […] to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services” or face fines of up to €20 million or 4% of annual global turnover – whichever is the greatest.

The GDPR is the latest step in the ongoing global recognition of the value and importance of personal information. Although the information economy has existed for some time, the real value of personal data has only become more recently evident. Cyber theft of personal data exposes EU citizens to significant personal risks. Big data analysis techniques enable organisations to track and predict individual behaviour, and can be deployed in automated decision-making. The combination of all these issues, together with the continuing advance of technology and concerns about the misuse of personal data by governments and corporations, has resulted in a new law passed by the EU to clarify the data rights of EU citizens and to ensure an appropriate level of EU-wide protection for personal data.

The GDPR applies across all the Member States of the EU but its reach is far wider: any organisation anywhere in the world that provides services into the EU that involve processing personal data will have to comply. This means that the GDPR is probably now the most significant data
security law in the world. While it builds on the work of the EU’s Data Protection Directive (DPD), the US’s HIPAA and various other data protection regimes, the GDPR can be regarded as a distillation and comprehensive update of the EU’s goals in protecting the rights and freedoms of the people who live within it.

The purpose of the GDPR

The DPD (Data Protection Directive) has been in place for twenty years; it sets a minimum standard for data protection law in EU Member States. Many states have gone significantly further in terms of legislating to protect personally identifiable information (PII), and this has made it increasingly difficult for EU citizens to know how their rights are protected across the EU and for organisations to determine which set of laws they should comply with, particularly when trading across multiple Member States.

The EU Commission therefore decided that a single, unified law would be a more effective way of achieving two key goals:

1. Protecting the rights, privacy and freedoms of natural persons in the EU.
2. Reducing barriers to business by facilitating the free movement of data throughout the EU.

In terms of EU legislation, a regulation is quite distinct from a directive, which is how data protection was previously handled under the DPD. While directives set minimum standards and then ask EU Member States to provide their own legislation to meet those standards, regulations exist as
Introduction

laws themselves, superseding any relevant laws passed by Member States.

While Member States are allowed to apply directives in whatever way suits each member, a regulation is applied consistently in all Member States. If there is room for local variations, it is specifically identified in the text of the regulation. Regulations are, therefore, an effective mechanism for applying a consistent approach across 350 million people in 28 Member States – and often beyond.

Structure of the Regulation

Appendix 1 of this manual provides a breakdown of the overall structure of the Regulation. The regulation itself can be downloaded, in all the official languages of the EU, from http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf. There is also a pocket guide to the EU GDPR, available from IT Governance Publishing\(^1\), which gives an overview of the legislation.

The GDPR is divided into two broad sections, which is standard for EU directives and regulations. The first section comprises the recitals. The recitals essentially provide context, direction and guidance so that the later explicit requirements can be better understood.

The second part of the Regulation comprises the articles. The articles set out the specific requirements with which those entities within the scope of the regulation have to comply.

---

\(^1\) [www.itgovernance.co.uk/shop/product/eu-gdpr-a-pocket-guide](http://www.itgovernance.co.uk/shop/product/eu-gdpr-a-pocket-guide)

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Introduction

Not every article in the GDPR applies to every organisation – given that some articles are relevant only to the Commission, the Board or the supervisory authorities, it may actually be impossible for every article to apply to a single organisation. In many cases, only a few articles may be completely relevant.

In broad terms, Chapters VI, VII, X and XI of the GDPR talk primarily about the Commission and the supervisory authorities so, if you are using this manual to plan your GDPR compliance programme, you may not need to give extensive attention to those sections.

Impact on the EU

As an EU regulation, the GDPR operates above the level of other Member State laws. It cannot be simply overturned or repealed by a single government or nation, nor can those governments or nations modify the legislated requirements to make compliance simpler or less effective. This is because it has already been agreed by representatives from all Member States through the standard EU legislative process.

The GDPR asserts a number of rights for individuals in relation to their personal data, and these rights are set out in Chapter III of the Regulation. The protection of these rights naturally results in a number of obligations on the part of the organisations that collect, store and process that personal data. Data collectors and processors have to act in accordance with the GDPR in order to ensure that the fundamental data rights of individuals are protected. This is not a simple “if A then B” law, of course, and there are various conditions that protect businesses’ rights to do
business, as well as protecting public authorities’ ability to serve the public.

On one hand, the Regulation appears to be disruptive. Every organisation in the EU has to comply with the law and that means they will all need to review the impact of the Regulation on their operations to determine what changes have to be made and the extent to which spending on compliance needs to be increased; there will have to be significant changes to how most organisations collect, process and store personal data; and the GDPR is, of course, bolstered by the threat of punitive and “dissuasive” administrative fines. On the other hand, the Regulation is trying to tread a fine line between protecting the rights of the individual and removing barriers to the “free movement of personal data within the internal market”. In other words, while the GDPR sets out specific restrictions on the use and storage of personal data, it does so in order to preserve the interests both of the EU’s residents and the organisations that do business within it.

Organisations that act quickly to ensure compliance with the Regulation will be those that thrive in the evolving regulatory environment. Equally, some organisations will be able to make significant process improvements, as with standardised requirements for data protection, organisations can streamline their processes – particularly for pan-EU and Internet services operations – and significantly improve efficiency.

Implementing the GDPR

The prerequisites for implementing a complex compliance framework are knowledge and competence; the IBITGQ
Introduction

(www.ibitgq.com) Certified EU GDPR Foundation and Practitioner qualifications are designed so that individuals can gain the skills and competence they need and this manual, the primary purpose of which is to help organisations tackle the GDPR, is also the text book for the IBITGQ EU GDPR Practitioner qualification.

This manual explains how to achieve compliance with the Regulation and how to do so while minimising the impact of the necessary changes. In any compliance project, there are many instances where organisational processes must be structured to meet legal or regulatory requirements, and it is important to ensure that your organisation is able to do this cost-effectively and efficiently.

It is also important to understand that the GDPR will apply in varying measures to organisations outside the EU. Much as you are expected to abide by the laws of any country you live in, non-EU organisations that provide services into the EU, where those services involve processing personal data, will also need to abide by the Regulation. While compliance with the Regulation may be difficult for some organisations – typically smaller ones that have no other interest in the EU – simple supply-chain forces, and the explicit GDPR requirements around extra-territorial data processing will put compliance pressure on organisations that want to do business within the EU.

In fact, the only real way to avoid complying with the GDPR will be to avoid doing business with the EU entirely. Given that the EU is the largest trading bloc in the world, this would be impractical for any organisation that wants to take advantage of the Internet or works with modern global markets and supply chains.
Introduction

This book does not lay out a one-size-fits-all framework for achieving GDPR compliance. Organisations operate in different ways, with different partners and suppliers, different business objectives and a variety of business models, and no single compliance framework is likely to work – or even be suitable as a general approach – for all organisations in all parts of Europe or the world. Rather, this book provides information about the features of a compliance framework that are known to work in many organisations and which reflect the GDPR requirements. The manual identifies the specific requirements of the GDPR and provides analysis and recommendations for pragmatically and effectively achieving compliance.

Readers should, however, note that this manual does not cover every possible situation in which the GDPR might apply, nor does it deal with the compliance requirements in every sector and industry. It instead focuses on the core activities and issues that most GDPR compliance projects are going to have to face, and provides advice and guidance that is broadly applicable in most – but not all – circumstances.

Finally, it should be noted that this is a manual for implementing a GDPR compliance framework in an organisation; it is explicitly not a legal compliance manual and you will need specific legal advice on aspects of the GDPR, particularly in relation to contracts and other legal statements. Your legal advisers have an important role to play in your GDPR project, but most lawyers are not experts on cyber security, information assurance or business continuity, nor do they usually have expertise in organisational management. Direct their services to the maximum value of your GDPR compliance project and remember that GDPR compliance is much bigger and more
important than legal documentation; the GDPR has to become part of the fabric of the organisation in much the same way as does Health and Safety, internal control or information security.

Key definitions

There are a number of key terms that are used throughout the manual, many of which have very specific definitions. These definitions all originate in the GDPR itself. Article 4 of the GDPR contains all the key definitions and should be thoroughly reviewed. Of these, there are five terms universally applied throughout the Regulation that need to be clearly understood from the outset.

**Processing**

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.\(^2\)

\(^2\) GDPR Article 4, Clause 2
Introduction

Controller

‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.3

The data controller is the organisation that determines the purpose for processing personal data and what processing will be done. As we’ve seen, “processing”, under the terms of the GDPR, includes collecting and storing information, so it’s possible that an organisation may be accountable as a controller but not otherwise involved with the actual processing of personal data. For a consumer products company that hires a marketing agency to profile their customers, and which provides the marketing company with the specific data necessary to provide those profiles, it will clearly be the data controller, and the marketing agency will be the data processor. If, however, the marketing agency determines what customer data it needs to see, and how that data will be used, and simply provides summary information to the consumer products company, then the marketing agency will be the controller.

3 GDPR, Article 4, Clause 7.

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Introduction

Processor

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.4

Data processors are organisations or entities that process personal information on behalf of a data controller. As noted above, “processing” is essentially anything done to the data, including storage, archiving, or just looking at it. It is normal for an organisation to be both a controller and a processor in respect of most personal data; it is only processing that is carried out by third parties on behalf of the controller that has to be addressed in line with the requirements on processors.

Personal data

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.5

Personal data under the GDPR is a broad set of types of information about “an identified or identifiable natural

4 GDPR, Article 4, Clause 8.
5 GDPR, Article 4, Clause 1.

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
Introduction

person”. This means that the information is not personal data if there is no way to link it to a natural person. Personal data is anything that could be linked in any way to the data subject, so organisations will need to be careful about how information is gathered and used, as it may be possible to accidentally gather sufficient information to remove the anonymity of the subject. Note that the definition now specifically includes biometric, genetic and health information, as well as online identifiers, such as an IP address that can be used to identify a person. The GDPR does not extend any rights to deceased persons.

Supervisory authority

‘Supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51.6 The supervisory authority is the governmental organisation in each Member State that will be responsible for enforcement of the GDPR. Your organisation may need to interact with the supervisory authority on a number of occasions, so it’s worth making sure you know who that will be (in the UK, for instance, it’s the Information Commissioner’s Office, while in France it is the Commission Nationale de l'Informatique et des Libertés, and so on). There is a full list of the current EU/EEA national supervisory authorities in Appendix 2.

6 GDPR, Article 4, Clause 21.

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
If your organisation operates in more than one Member State, you may have a lead supervisory authority in whichever Member State the main establishment of your organisation is based\(^7\).

\(^7\) GDPR, Article 56

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
CHAPTER 1: PRIVACY COMPLIANCE FRAMEWORKS

The first few steps of your compliance project can be the most confusing. Where do you start? Who needs to be involved? How do you go about identifying and meeting all of your obligations? How will you prove that you’re meeting all of the Regulation’s requirements?

Such questions can distract you from the project’s core requirements and make the entire process seem incredibly daunting.

For most organisations, a simple approach may be to ignore the specific, detailed requirements of the GDPR for now, and start instead by building a framework to ensure compliance both now and in the years ahead. The GDPR has a specific requirement that controllers should, “taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, […] implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

This clause is, in effect, saying that organisations should put in place a compliance framework that ensures they are implementing appropriate technical and organisational

---

8 GDPR Article 24, Clause 1.
measures to ensure that data processing is performed in compliance with the GDPR.

The GDPR also explicitly requires organisations to demonstrate that they have embedded the principle of ‘data protection by design and by default’ into their organisational culture. Although there are a number of specific steps necessary to embed data protection by design, the starting point is undoubtedly to create an appropriate compliance framework that makes sure that data protection is in reality at the core of the organisation’s behaviour.

A “compliance framework” is a structured set of guidelines and practices that bring together the regulatory compliance requirements that apply to an organisation, and the business processes, policies and controls that are necessary in order to meet these requirements. Technical measures include specific procedures, as well as staff training, audits and all the relevant technical and physical security controls that form part of an effective information security management system. These processes, policies and controls will generally outline how the organisation manages communication, risk and governance relevant to the compliance requirements. Because there will often be some overlap between different compliance requirements, the framework should identify this in order to eliminate redundancies and uncertainties.

All compliance frameworks have to include three categories of activity as illustrated in Figure 1: people, process and technology.
A compliance framework could be developed for any set of legislative, regulatory or contractual requirements. For the GDPR, of course, it will be a privacy compliance framework. The development of a privacy compliance framework is comparable to any other ongoing business project; you want to establish a set of practices and policies that make sure that certain processes are always followed. Assuming those processes are aligned with the legal requirements, the framework should ensure that the organisation remains on the right side of the law. Importantly, all the necessary processes don’t need to be defined from the start: they can be built into the framework at appropriate stages in order to achieve compliance. The most important step is getting the initial framework in place.
1: Privacy Compliance Frameworks

There are two ways of approaching this task: work it all out for yourself, or deploy and adapt a publicly available compliance framework. The first option relies on some combination of trial and error and (probably expensive) consultancy support; the second draws on established best practice and can be a faster and more cost-effective route to compliance than doing it all yourself.

There are several compliance frameworks and standards to choose from. The GDPR explicitly identifies the use of international standards and privacy marks as effective tools for demonstrating compliance with requirements and it makes practical and commercial sense for a privacy compliance project to start off by drawing on such established best practice.

A privacy compliance framework is useful primarily because it provides a structured way of managing confidential data in such a way that the organisation is able to comply with often complex laws and, perhaps, on a multi-jurisdictional basis. Organisations that do not already have a privacy compliance framework can use a standardised framework to make the leap from exposure to compliance; organisations that do already have a privacy compliance framework can use national and international standards to obtain certifications that will enhance credibility with customers and stakeholders while also demonstrating to regulators and, perhaps, judges the due diligence and compliance efforts that have been made. There are currently two recognised standards or frameworks that could be used: ISO/IEC 27001:2013 and BS 10012:2017. There is an internationally recognised, accredited certification programme for ISO 27001. The certification status for BS 10012 is not yet clear. Other standards and Trust Marks are also expected to emerge.
The three key areas of a privacy compliance framework are:

- governance, risk management and compliance objectives;
- the data protection principles;
- policies, procedures, controls and records.

In most management systems and frameworks, there is a sense that the various processes are related, and that they feed into and are informed by a common set of controlling processes. That is, like most business processes, these functions will have defined inputs and outputs, and the privacy-specific inputs will eventually result in privacy-specific outputs.

**Material scope**

Any framework applies to a specific scope, the area of the organisation and its operations that fall within it. For the purposes of compliance, the scope of the framework must be directly informed by the requirements of the Regulation, which is described in Article 2.

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.\(^9\)

---

\(^9\) GDPR, Article 2, Clause 1.

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
That is, your framework must cover all activities that involve the collection, use or other processing (such as deletion or modification) of personal data. For many organisations, this will cover almost all of their activities. Remember that this does not specify that the personal data is that of customers: you must also include personal data of your employees, contractors, etc.

There are some exemptions, but these typically relate to either high-level Union activities (such as Member States operating in the interests of national or Union security), in the pursuit of criminal justice by competent authorities, or to very low-level activities (such as handling personal data as a natural person exercising activities that are exclusively personal or domestic, rather than as an organisation processing in pursuit of business objectives).

**Territorial scope**

The GDPR is explicit in saying that it applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

---

10 GDPR, Article 3.
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In other words, any organisation in the world may be subject to the GDPR if it provides services to data subjects that are within the EU. Please consider Recital 14: “the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data”. GDPR confers the same rights on all data subjects, wherever in the world they may live, if that data is processed by a controller or processor within the EU or by one that is providing services into the EU. This may have significant implications on the scope of organisational privacy compliance frameworks.

Furthermore, the GDPR requires organisations that are based outside the EU to nominate in writing a representative organisation within the EU. This representative must be located in one of the Member States where the target data subjects are based and must be mandated by the data controller or data processor to be addressed by the supervisory authority or data subjects on all issues relating to the processing of personal data. The appointment of such a representative will not, however, enable the controller or processor to avoid legal action for breaches of the GDPR.

In terms of the compliance framework, there may be other considerations, such as local or sector-specific laws and regulations, that may also have to be taken into account.

---

11 GDPR, Article 27.
Governance

All organisations have an obligation to comply with the law. One of the fiduciary duties of directors is to ensure that their organisation has taken appropriate steps to comply with all relevant laws. Directors also have a fiduciary – and in many cases also a legal and contractual duty – to ensure that risks to the organisation are appropriately managed. Cyber risk is an example of the type of risk of which directors have to be aware. Cyber attack exposes organisations to significant reputational and operational damage, as well as the possibility of legal action by those whose personal data has been compromised. The GDPR gives any data subject the right to pursue judicial remedies for both material and non-material harm arising from the processing of their data. This, combined with the specific GDPR requirements around data breach reporting and the significant administrative penalties for compliance breaches (up to 4% of global revenue or €20 million, whichever is greater), should be on the radar of all directors and on the agendas of all board meetings. Boards should ensure that the privacy compliance frameworks that are put in place are capable of ensuring GDPR compliance and that they contain mechanisms for providing regular reports and assurance to the board on the state of compliance across the organisation.

One way that boards can approach their governance responsibility in respect of information and privacy risk is through the appointment of a board-level senior information risk owner (or ‘SIRO’). The UK Government originated the idea of this role as part of its extended strategy to tackle information risk across the public sector and described the role of SIRO to be managing information risk from a business not a technical perspective, focusing on the strategic...
information risks related to the delivery of corporate objectives. This means taking a holistic approach to information risk across the supply chain and managing it in line with the organisation’s risk appetite. This is a useful role for a board to put in place. This role is expected to work with board colleagues to:

1. establish an information risk strategy which allows assets to be exploited and risks to be managed effectively;
2. identify business-critical information assets and set objectives, priorities and plans to maximise the use of information as a business asset; and
3. establish and maintain an appropriate risk appetite with proportionate risk boundaries and tolerances.

Clearly this role has a broader responsibility than simply managing privacy risk. The reality, however, is that any framework you build to manage privacy risk must, perforce, be part of your wider framework for managing information risk. It therefore makes sense to tackle GDPR compliance as part of your wider strategy for managing information risk.

This governance element should manifest itself in appropriate resource commitment – in terms of personnel, financing and systems – to the GDPR compliance project, in demonstrable top management leadership and commitment, and in the corporate privacy policy and throughout internal communications.

All international management system standards published after 2013 contain, in clause 5 and its sub-clauses, a number of specific requirements covering top management commitment; these provide a good starting point for any
organisation in determining the leadership of a corporate governance framework. The clause 5 requirements are detailed below.

Top management demonstrates leadership and commitment to the management system by:

a. ensuring policy and objectives are established and are compatible with strategic direction;
b. ensuring integration of the management system into the organisation’s processes;
c. ensuring resources needed for the management system are available;
d. communicating importance of effective management and of conforming to the management system requirements;
e. ensuring the management system achieves its intended outcome(s);
f. directing and supporting persons to contribute to the effectiveness of the management system;
g. promoting continual improvement, and;
h. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

ISO/IEC 38500 is a standard that deals specifically with the corporate governance of information and communications technologies. It, too, is useful guidance for creating an effective technology governance framework.
Objectives

Your privacy framework will have a number of objectives. Obviously, the overall objective should be to comply with the Regulation and to avoid the “dissuasive” fines and other punitive measures. Your framework should also identify specific subsidiary objectives relating to the rights of data subjects and the protection of personal data.

Objectives should be determined in a way that enables performance against them to be tracked and measured. An objective is only useful, after all, if you can determine how you stack up against it. The normal acronym used in relation to objectives is that they should be SMART:

- Specific
- Measurable
- Actionable (or achievable)
- Realistic
- Time-bound

The performance of information security controls should be capable of measurement and improvement and ISO/IEC 27004 provides specific guidance on control measurement. While this standard is a useful starting point for tackling control performance, it does not contain specific guidance on measuring performance against specific data privacy objectives.

Key objectives could include:
• the capability of responding to subject access requests within the new prescribed time frame (now one month\(^\text{12}\));
• the capability of identifying and reporting data breaches to supervisory authorities within 72 hours;
• retention periods of personal data;
• staff awareness training.

Key processes
A privacy framework should have a number of key processes, some of which your organisation may already have, and others that may be new. These could include processes for incident management, change management, corrective action, risk management and continual improvement.

Incident management processes – which will be discussed in Chapter 14 of this manual – are all about what you do when there is a data breach or some other information security incident.

Fundamentally, the incident management process will comprise several stages: realising that something has happened and reporting it, understanding what has happened, containing the event to minimise damage, repairing the damage, making sure that the event cannot recur, and reviewing the organisation’s response. The outputs of the

\(^\text{12}\) GDPR, Article 12.
The organisation will also need **change management** processes. All organisations have to change and adapt to risks and events, and to changes in customer and market requirements. When changes are rolled out to an organisation in an unstructured manner, new and unforeseen risks can be introduced. This is particularly true of ICT-related processes. Inadequate management of changes to business processes (or to departments or reporting structures) can create risks to personal information and possible breaches in existing privacy protection mechanisms. A change management process is an essential step in ensuring that rolling out a change is completely thought through, that possible deviations, problems and consequences have been identified and mitigated, and that roll-back options are in place.

A **corrective action** process is also necessary so that an organisation can make amends when something doesn’t work as intended. This might be as obvious as a control being inadequate and failing to suitably protect an asset, or it might be a larger, systemic fault that prevents a whole process from functioning. In either case, the organisation will need a systematic method of identifying and remediating the fault.

You’ll see the obvious connection here with the incident management and change management processes. Once an incident has been dealt with, there should be an analysis of the cause of the incident, which should lead to the identification of amendments to or changes in existing controls or processes. These changes should be dealt with through the corrective action process, ensuring that corrections are reviewed and approved, that they’re correctly
1: Privacy Compliance Frameworks

implemented, and that they’re reviewed for effectiveness. This last point is worthy of note: a corrective action needs to correct the problem, so your process will need to include a review stage. This review might be a one-off confirmation or it might require ongoing attention – that’s something the process will need to identify.

One of the more critical processes is risk management, which is dealt with in much greater depth in Chapter 6 of this manual. All organisations face risks and, in the case of GDPR compliance, the focus will be on risks to personal data and to the systems and processes that interact with that data.

Risk management is very much at the core of any privacy compliance framework because the organisation needs to understand exactly what risks it needs to protect itself from. Just as a person might put on a suit of armour to save themselves from injury, that suit will be completely useless against poisonous gas, or might only have limited effectiveness against a bear. The organisation should ensure it invests its money and resources in the right areas, so having an effective risk management regime in place is a good way of ensuring that the return on investment is worthwhile.

Where privacy risk is concerned, though, the risk management programme must also look closely at risks to the ‘rights and freedoms of natural persons’ that might arise from the processing of their data. In a sense, the GDPR says to organisations that they face the risk of substantial administrative fines, as well as legal action from data subjects, if they fail to adequately manage risks to those data subjects.

A framework or management system should also have an underlying continual improvement process. A continual
improvement process assesses existing processes and their outputs for conformity with laws, regulations or other requirements, determines any necessary adjustments, and then feeds these into the originating processes that determine the framework or management system’s inputs. In simpler terms, you might like to refer to the Plan-Do-Check-Act cycle (PDCA, also called the Deming Cycle), which is a popular management tool for ensuring ongoing improvement.

Other continual improvement cycles, such as the COBIT® Continual Improvement Life Cycle or the ITIL® Continual Service Improvement process, could be applied instead of the PDCA cycle.

The PDCA cycle divides the standard processes and practices for a management system or development process into four distinct stages: planning, doing, checking and acting. As a cyclical process, each stage feeds into the one that follows and enables continual improvement.

In brief:

• the organisation plans what it is going to do;
• does what it has planned to do;
• checks whether what it has done has achieved what it planned, and;
• acts on those findings to improve how it achieves its objectives.
The PDCA cycle is illustrated in Figure 2, below.

Understanding how the processes and continual improvement of those processes all fit together is a critical feature of any effective compliance framework. Under the assumption that all of your processes are adequate and that they are being followed, such a framework provides assurance that you are continuing to adapt and improve your processes so as to continue meeting your compliance requirements.
1: Privacy Compliance Frameworks

Personal information management systems

Personal information management systems (PIMS) are a form of management system dedicated to the management of personal information. As such, they can form a good basis for a compliance framework.

It is important to note that, while a PIMS and a compliance framework are broadly similar, there are distinctions. For instance, a compliance framework is not necessarily a “single object” but may be comprised of two or more management systems working in concert (a PIMS and an information security management system, or ISMS, for example). A PIMS may also be focused on simply managing personal information rather than necessarily protecting it in line with legal or regulatory requirements. In this sense, the PIMS may only provide some of the processes necessary to ensure overall compliance.

While a PIMS is not necessarily designed to ensure compliance with the GDPR specifically – or even with current laws such as the UK’s Data Protection Act (DPA) or Germany’s Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) – standardised models will usually include a requirement to identify legislative, regulatory and contractual requirements relating to personal information, and to include those requirements in the PIMS.

There are several possible ways to achieve this and BS 10012:2017 – *Data protection – Specification for a personal information management system* – provides one such framework for doing so. It provides a well-defined, well-understood structure for managing data protection, and it is designed to follow the PDCA cycle to ensure continual improvement. While the earlier version of the standard was
1: Privacy Compliance Frameworks

Specific to the UK’s DPA, it has been re-drafted and updated to reflect the requirements of the GDPR and, as such, BS 10012: 2017 should be generally suitable as the core of a privacy compliance framework.

BS 10012 includes a requirement to “define the scope of the PIMS and set personal information management objectives, with due regard to the […] applicable statutory, regulatory, contractual and/or professional duties”13. Properly applied, this means that the processes described in BS 10012 should take the appropriate legal requirements into account.

However, BS 10012 may not on its own be an adequate framework, depending on how your organisation collects, stores and uses personal data. BS 10012 is narrowly focused on privacy protection, and if personal data is more widely used across your business processes, then a more comprehensive security framework would be appropriate. In this circumstance, you may need to define additional processes in order to comply with the Regulation. This is where an additional management system may be useful, such as ISO/IEC 27001, which is the international standard that describes best practice requirements for an information security management system (ISMS).

Regardless of the standard or business process model employed, a PIMS is likely to be a useful core for your privacy compliance framework. Figure 3 provides an overview of the typical components of a PIMS.

13 BS 10012:2009, Clause 3.2 d).

This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
ISO/IEC 27001:2013

The GDPR requires organisations to go further than simply putting in place a PIMS. There is an explicit requirement\textsuperscript{14} for organisations to have in place:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

\textsuperscript{14} GDPR, Article 32, Clause 1 – Security of Processing.
1: Privacy Compliance Frameworks

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This really does mean that organisations have to integrate data and privacy protection into ‘business as usual’ and that a more comprehensive approach to information security – one which deals with the processing systems and services, as well as with security, continuity and continual security testing (primarily in the form of penetration testing) – is essential. This is where ISO/IEC 27001 comes in.

ISO 27001 is an internationally recognised, management system standard for information security management. It describes the requirements of an information security management system (ISMS) based on established best practice. It is sector-agnostic, does not favour any one technology or solution, and can be used by organisations of any size. It sets out requirements for what must be done to secure information but provides room for organisations to determine how they implement the requirements to meet their organisational objectives and risk appetite.

This framework for information security can also be used to achieve accredited external certification. The assurance provided by such certification is widely recognised as proof that the organisation protects information assets, and it is a requirement in a growing number of contracts that involve valuable information.

Structurally, it’s not too different from BS 10012; both describe processes that are critical to the protection of personal data, and both recognise that a number of processes are necessary to assure the security of this data. The distinction is that BS 10012 is specifically focused on
personal information, while ISO 27001 is interested in information more generally. As such, an ISO 27001 ISMS could be used as a larger framework within which BS 10012 can sit. ISO 27001 encourages the organisation to seek out additional sources of best practice, and BS 10012 is certainly that.

Figure 4 shows the structure of an ISO 27001 ISMS.

ISO 27001 aims to safeguard the “confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested
parties that risks are adequately managed”\textsuperscript{15}. In fact, information security is defined as the “preservation of the confidentiality, integrity and availability of information”. In information security:

- Confidentiality is the “property that information is not made available or disclosed to unauthorized individuals, entities, or processes”\textsuperscript{16};
- Integrity is the “property of accuracy and completeness”\textsuperscript{17};
- Availability is the “property of being accessible and usable upon demand by an authorized entity”\textsuperscript{18}, and;
- Risk is the “effect of uncertainty on objectives”\textsuperscript{19}.

Confidentiality, integrity and availability are often called the CIA of information security, because they’re the key attributes of secure information. The GDPR itself mentions them explicitly on a number of occasions. Similarly, ISO 27001’s approach to risk is in alignment with the Regulation’s requirements for impact assessments, as you’ll see later in this manual.

ISO 27001 takes the approach that information security must be driven from the top down. As such, it contains the

\textsuperscript{15} ISO/IEC 27001:2013, Clause 0.1.
\textsuperscript{16} ISO/IEC 27000:2016, Clause 2.12.
\textsuperscript{17} ISO/IEC 27000:2016, Clause 2.40.
\textsuperscript{18} ISO/IEC 27000:2016, Clause 2.9.
\textsuperscript{19} ISO/IEC 27000:2016, Clause 2.68.
requirement that an information security policy, signed off by top management, is enacted through critical processes such as risk management, monitoring and review, corrective actions, and so on.

ISO 27001 Annex A lists 114 controls, in 14 categories, which can be used to identify what may be appropriate controls to help manage the security of personal information. Figure 5 shows the 14 control categories.

Figure 5: The 14 control categories of Annex A

The best book for detailed, practical guidance on implementing these controls is Alan Calder and Steve Watkin’s *IT Governance: An International Guide to Data*
1: Privacy Compliance Frameworks

Security and ISO27001/ISO27002\(^20\), now in its sixth edition. For a straightforward description of how to design and implement an information security management system that meets the requirements of ISO/IEC 27001:2013, turn to Alan Calder’s *Nine Steps to Success: an ISO27001 Implementation Overview*\(^21\). IBITGQ also has relevant ISO 27001 implementation and audit qualifications available.

Organisations that implement ISO 27001 will naturally find themselves accruing evidence of their compliance to the Standard, especially if it has gone to the trouble of external certification for their ISMS. This evidence is useful beyond simply getting certification or showing clients that your processes are secure. In the event that an organisation is subject to an investigation or audit, it will be able to draw upon this evidence to show that it has been following best practice, that it has taken appropriate steps to prevent incidents, that it recognises the risks it faces, and that people at all levels throughout the organisation are appropriately trained, competent and responsible.

**Other standards**

While ISO 27001 and BS 10012 are the most likely candidate standards to use as the basis of a privacy compliance framework, there are other standards and business process models which could also be used. Whichever you choose –


This extract and the original text it is taken from our both subject to ITGP copyright and may not be reproduced, in any form, without prior written consent from the publisher.
and whether you decide to choose one of the standards or business processes mentioned here – will depend on your organisation and its specific processes, resources and requirements.

COBIT® (Control Objectives for Information and Related Technologies) is a control-based framework for the governance of IT and information. It may seem a slightly abstract approach to GDPR compliance, but establishing governance and oversight will be an important part of ensuring the security and privacy of personal data, as will asserting accountability and responsibility for maintaining this. COBIT is a widely used framework in some countries – particularly at the enterprise level – and so there are publications and experts available to provide advice and guidance, if necessary.

Other frameworks have been developed by government agencies to simplify the compliance process when working with complex sets of legislation. While these may not be immediately relevant to GDPR compliance, they often contain an effective structure and processes that can be applied to meet European compliance requirements. The Privacy Management Framework22 developed by the Office of the Australian Information Commissioner (OAIC), for instance, is a simple four-stage process that matches the PDCA cycle, and provides guidance at each stage to ensure compliance with the range of Australian law and other

relevant requirements imposed by other nations that Australia regularly trades with.

The US National Institute of Standards and Technology (NIST) has also built an extensive collection of information security standards, known as the NIST Special Publication 800 series. While it is not specifically an information security management framework, the NIST SP 800-53 model is used by US government agencies that need to comply with the requirements of Federal Information Processing Standard (FIPS) 200. Although NIST SP 800-53 may be intended for government agencies, the framework could certainly be applied to other industries.
Buy your copy today!


